(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 762 692 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
12.03.1997 Bulletin 1997/11

(51) Int Cl.[6]: **H04L 9/32**, G07B 17/04

(21) Application number: **96113397.2**

(22) Date of filing: **21.08.1996**

(84) Designated Contracting States:
DE FR GB

(30) Priority: **21.08.1995 US 518404**

(71) Applicant: **PITNEY BOWES INC.**
Stamford Connecticut 06926-0700 (US)

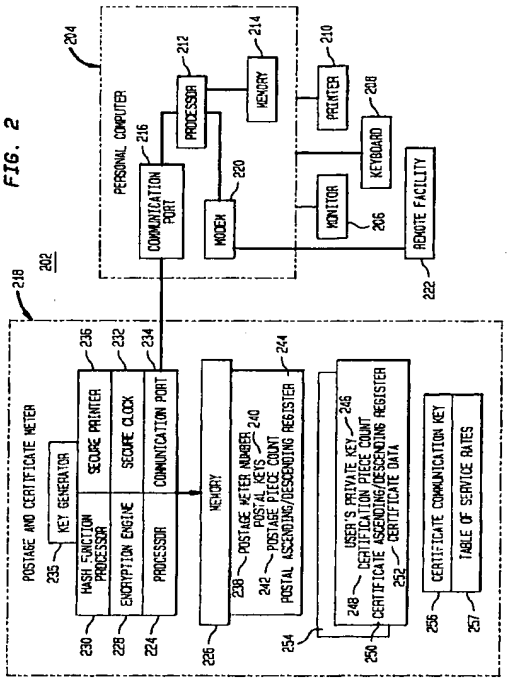
(72) Inventors:
- **Cordery, Robert A.**
  Danbury, Connecticut 06811 (US)
- **Lee, David K.**
  Monroe, Connecticut 06468 (US)
- **Pintsov, Leon A.**
  W. Hartford, Connecticut 06107 (US)
- **Ryan, Frederick W., Jr.**
  Oxford, Connecticut 06478 (US)
- **Weiant, Monroe A., Jr.**
  Trumbull, Connecticut 06611 (US)

(74) Representative: **Avery, Stephen John et al**
Hoffmann, Eitle & Partner,
Patent- und Rechtsanwälte,
Arabellastrasse 4
81925 München (DE)

(54) Secure user certification for electronic commerce employing value metering system

(57) A system and method include means for processing a cryptographic certificate adapted to provide security functionality. A register means (244) is provided and means (224) for adjusting the register means to account for services when the cryptographic certificate is processed. The register means may be for storing funds. Means are provided for processing a digital token providing proof of postage payment and means are also provided for processing a cryptographic certificate adapted to provide security functionality. Funds stored in the register means are debited when the digital token is processed and when the cryptographic certificate is processed. Processing the cryptographic certificate may involve many functions such as providing security services and/or certificate management functions (including generating and verifying cryptographic certificates) and/or key management functions and/or access to any needed private keys to perform security services. Processing the digital token may include generating the digital token or issuing the digital token.

FIG. 2



EP 0 762 692 A2

Description

The present invention pertains to certification of users for electronic commerce, and more particularly, to a secure user certification system for electronic commerce that provides an accounting system for services provided.

In electronic commerce various parties conduct activities without face to face contact. Accordingly, it becomes desirable for each party to any given transaction to be able to determine and verify the authenticity of the other party to the transaction.

Each user can authenticate messages from the other party by the use of a certificate digitally signed by a trusted third party. The critical part of the user's certificate is the user's public key. The authenticity of the certificate can be established by verifying the digital signature of the trusted third party. A message from the user can be authenticated by verifying that it has been digitally signed using the private key matching the public key in the certificate.

A transaction may also require security services. These may include, for example, message integrity, message authentication, message confidentiality, and message non-repudiation. The meaning of the message integrity is, that the message has not been altered. Message authentication is that the message is genuine and was signed by the other party. Message confidentiality is that the message contents are available only to the authorized parties to the transaction and no other parties. And finally, message non-repudiation is that the initiator of the message is unable to repudiate at a later time that the message originated with such party.

In a traditional paper based transaction, the above security services are normally implemented by means of signature, seals, stamps and the like. In an electronic commerce environment these security services are achieved by cryptographic techniques such as digital signature, hash codes, encryption algorithms, and the like.

In order to effectively implement the above security services, a party to an electronic commerce transaction, must have access to a secure cryptographic device capable of securely implementing these cryptographic techniques.

It should be recognized that various protocols have been designed to implement the above mentioned security services. An example of this is set forth in Section 2.1 of the US Department of Commerce document entitled Standard for Public Key Cryptographic Entity Authentication Mechanism, Draft, March 13, 1995, Federal Information Processing Standards Publication JJJ. Public key cryptography algorithms including RSA and algorithms based on Elliptic Curves are used to encrypt, authenticate, and verify integrity of messages. Message digests are generated with algorithms including MD5 and the Secure Hash Algorithm (SHA).

It is known that to enable the above types of cryptographic services, a set of keys is needed. This can be a set of secret keys (for a secret key system) and/or public and private keys (for a public key system). The secret and private keys have to be securely communicated or otherwise provided to a user and thereafter protected.

Public key cryptographic certificates, Certificate Authority and Certificate Management are also known and are the subject of standards. For example ANSI standards X.509 deals with Certificate Management and X. 9.30-3 describes Certificate Management for Digital Signature Algorithm. Secure cryptographic Certificate Management devices are known that utilize public key cryptography to verify certificates of public keys, and use the private portion of the key to authenticate documents, transactions, and communications and perform other cryptographic functions. Various enterprises have proposed being a Certificate Authority, for example, the United States Postal Service has proposed entering into electronic commerce as a Certificate Authority based on its acceptance as a trusted third party.

The present invention provides practical means of implementing certification processes achieving this goal for a large group of users on an economical basis.

An object of the present invention is to provide a convenient payment system for use in electronic commerce.

Another object of the present invention is to provide a convenient key management system for use in electronic commerce.

Postage meters are known that use secure cryptographic means to receive funds and to provide convenient secure evidence of postage payment; however, it has been discovered that various postage evidencing devices and systems have within them the capability of being modified to provide a broader security device functionality.

It has further been discovered that the postage evidencing devices enable a payment method for the services of the trusted third party.

A further object of the present invention is to utilize a postage or other value evidencing device to provide security services.

Still a further object of the present invention is to enable security services such as authentication, data integrity and confidentiality by utilizing the user's private and/or secret keys stored and protected in the value evidencing device.

Yet a further object of the present invention is to implement certificate management functions such as issue of certificates, certificate revocation and certificate verification within a value evidencing device.

An additional object of the present invention is to enable a payment system for the certificate management services provided by the trusted third party.

Yet an additional object of the present invention is to provide for inspection aimed at detection of key compromise carried out by tampering with a value evidencing device.

A system and method embodying the present invention include means for processing a cryptographic certificate adapted to provide security functionality. A register means is provided and means, connected to the register means and the processing means, for adjusting the register means to account for services when the cryptographic certificate is processed and/or when other security services are performed.

In accordance with another aspect of the present invention a system and method include a register means for storing funds. Means are provided for processing a digital token adapted to be imprinted on a mail piece as a proof of postage payment and means are also provided for processing a cryptographic certificate adapted to provide security functionality. Means are provided which are operatively connected to the register means and to both the digital token processing means and the certificate processing means, to debit funds stored in the register means when the digital token is processed and when the cryptographic certificate is processed.

Reference is now made to the following Figures wherein like reference numerals designate similar elements in the various views and in which:

FIGURE 1 is a public key certificate and private key helpful to an understanding of the present invention;

FIGURE 2 is a value metering system, here a postage metering and certificate metering system embodying the present invention; processing a cryptographic certificate includes the above mentioned certificate management functions and use of the private key to perform security services;

FIGURE 3 is a flow chart of the generation of a cryptographic postmark which may be associated with a message to be communicated by the system shown in FIGURE 2.

FIGURE 3A is a flow chart of the generation of a cryptographic postmark by an agent employing the system as shown in FIGURE 2;

FIGURE 4 is a flow chart of the validation of a cryptographic postmark as carried out by the system shown in FIGURE 2;

FIGURE 5 is a flow chart of the generation and installation of a certificate in the system shown in FIGURE 2;

FIGURE 6 is a flow chart of a process for revoking a certificate generated in accordance with the process shown in FIGURE 5;

FIGURES 7A and 7B are examples of various types of certificates which may be issued by the system shown in FIGURE 2;

FIGURE 8 is a flow chart of the process for receiving a line of credit by the system shown in FIGURE 2; and,

FIGURE 9 is a flow chart of payment from the line of credit implemented by the operation shown in FIGURE 8.

A postage and certificate meter provides certificate management services including use of cryptographically secured certificates issued by a certificate authority. As more transactions are occurring electronically, rather than by physical mail, between parties who do not meet each other personally, a trusted third party is needed. Postal services have an infrastructure, governmental authority, and responsibility for universal access that makes them a natural choice for a certificate authority although other third parties may also provide services and be a certificate authority. The present system provides significant advantage, because the postage and certificate meter is a secure, inspected cryptographic device that the postal service has licensed an authenticated entity to use. The device extends the use of the postage meter to electronic commerce applications without duplicating expensive infrastructure. Small charges for processing certificates including issuing certificates and for processing such as generating and verifying electronic certificates also referred to as electronic postmarks can be paid using funds stored in the meter.

A postage and certificate meter combines the functionality of a postage meter and a certificate management device, providing significant advantage to, the postal service (and other certification authorities) and to the user. The postage and certificate meter is a secure cryptographic device with secret information that allows secure communication with the certificate authority such as a post office or other trusted third party and capability to use, manage and execute various security services. The postage and certificate meter includes metering and accounting capability that allows convenient low cost payment of charges per use of a certificate.

Advantages to the postal service as a trusted third party or to any other trusted third party include: manage keys for fewer secure devices; increased use of existing meter tracking infrastructure; fewer devices to inspect; legal right to inspect already in place; provides secure communication channel between postage and certificate meter and certificate authority; produce authenticated messages for postal service regarding the status and usage of the meter, thus providing additional security and assurance for postal funds and certificate authority payments; use of the postage and certificate meter for postage payment provides ongoing assurance to the certificate authority that the device is operating correctly, and has not been abused.

Advantages to the user include: a single secure coprocessor to validate payment of certificate use charges and postage reduces the number of secure devices to

manage; a single account to pay for certificate usage and postage; postage and certificate meter can efficiently pay certificate authority charges for processing certificates including new certificates and for use of the certificate; secure installation, storage and use of the private portion of the certificate; and, secure revocation of certificates.

Reference is now made to FIGURE 1. A certificate 102 is a file of data containing certain information which provides a secure user certification useful in electronic commerce. The certificate 102, which may be an electronic file or a tangible file such as a printed document or smart card or the like, enables a certificate holder to engage in various commercial and other activities which require services of authentication, privacy, data integrity and non-repudiation. The certificate 102 includes an identification of the certificate holder and the certificate holder's public key, signed with the private key of the certification authority, usually a trusted third party.

The certificate data may include, for example, the unique name of the user, a serial number or certificate number, that is, a unique number associated with the certificate, the public key of the user, the identity of the certificate authority or issuer, the validity dates for the certificate and the authorized use of the certificate. The private portion of the user's key shown at 118 is maintained and protected by the postage and certificate meter for the user. It is understood that the user's private key is the private key matching the certificate's public key. When user wants to send a message, the message is signed with the user's private key. The recipient of the signed message verifies the authenticity of the sender's certificate using the certificate authority's public key, and subsequently verifies the authenticity of the message using the sender's public key which may be obtained from the certificate.

Reference is now made to FIGURE 2. A value and certificate metering system shown generally at 202 includes a personal computer 204 having a monitor 206, a keyboard 208, and is connected to a printer 210. The personal computer 204 additionally includes a processing subsystem 212 having an associated memory 214. The processor is connected to a communications port 216 for communication with a secure postage and certificate meter subsystem 218 and a modem 220 for communicating with a remote facility 222. It should be recognized that many variations in the organization and structure of the personal computer 204 as well as the postage metering and certificate metering subsystem 218 can be implemented. As an example, the communications from the modem to the remote facility can be by way of hardwire or can be by way of radio frequency communications or other communications. The postage and certificate metering subsystem take many forms, for example it may be a secure vault type system, or a secure smart card system.

The postage portion of the postage and certificate meter 218, for example, may be similar to any of numerous postage metering systems as for example the systems shown in postage metering systems which generate and employ digital tokens are described in U.S. Patent No. 4,757,537 for SYSTEM FOR DETECTING UNACCOUNTED FOR PRINTING IN A VALUE PRINTING SYSTEM, issued July 12, 1988; U.S. Patent No. 4,831,555 for SECURE POSTAGE APPLYING SYSTEM, issued May 15, 1989; U.S. Patent No. 4,775,246 for SYSTEM FOR DETECTING UNACCOUNTED FOR PRINTING IN A VALUE PRINTING SYSTEM, issued October 4, 1988; U.S. Patent No. 4,873,645 for SECURE POSTAGE DISPENSING SYSTEM issued October 10, 1989 and, U.S. Patent No. 4,725,718 for POSTAGE AND MAILING INFORMATION APPLYING SYSTEMS, issued February 16, 1988. These systems, which may utilize a device termed a postage evidencing device (PED), employ an encryption algorithm which is utilized to encrypt selected information to generate the digital token. The encryption of the information provides security to prevent altering of the printed information in a manner such that any change in a postal revenue block is detectable by appropriate verification procedures. Moreover the system for the cryptographic capability may employ systems and methods such as those disclosed in pending European Patent Application Serial No. 96105237.0 filed April 1, 1996, for CRYPTOGRAPHIC KEY MANAGEMENT AND VALIDATING SYSTEM, which is assigned to Pitney Bowes, Inc., the entire disclosure of which is hereby incorporated by reference.

The postage and certificate meter subsystem 218 includes a processor 224 coupled to a memory 226. The processor has associated with it an encryption engine 228, a hash function processor 230, a secure clock 232 and a communications port 234. A key generator 235 is also provided for generating keys for use by the postage and certificate mailer. If desired, either a secure printer or a non-secure printer may be connected to the postage and certificate meter subsystem 218, if a printing capability is desired. In the FIGURE 2, a secure printer is shown at 236. The memory 226 may have stored within it different data as well as the operating program for the postage and certificate meter subsystem 218. The data shown as stored in the memory include the postage meter serial number 238, postal keys 240, postage piece count 242, postage ascending/descending register 244. If the meter was a current account meter unit such as employed in certain European countries, the ascending/descending register would be only an ascending register. Current account systems may be employed in the present system.

Additionally stored within the postage and certificate meter 218 memory 226 are user's private key 246, certificate piece count 248, and certificate ascending/descending register 250. This register may be combined with the postage ascending/descending register. Other certificate data shown generally at 252 may also be stored in the memory as well as a certificate communi-

cations key 256. A Table of Services Rates is provided at 257. This table includes the rates for the various services that may be obtained when processing a cryptographic certificate and/or when processing a digital token. The rating system for the postage and certificate meter 218 may implement the system disclosed in U.S. Patent No. 5,448,641 issued September 5, 1995 for POSTAGE RATING SYSTEM WITH VERIFIABLE INTEGRITY, the entire disclosure of which is hereby incorporated by reference. As is shown by memory area 254, more than one certificate may be stored in the memory 226.

It should specifically be noted that processing a cryptographic certificate may involve security services and/or certificate management functions including generating and verifying cryptographic certificates and/or key management functions and/or access to any needed private keys to perform security services.

Reference is now made to FIGURE 3 depicting the generation of a cryptographic postmark. A cryptographic postmark is a datafile which may contain message digest, date, time and other data which may be required to provide security services. A message is generated at 302. The message may be generated in the computer 204 or elsewhere depending upon the particular needs of the user. A message digest is obtained at 304 employing the hash function processor 230 of the postage and certificate meter subsystem 218. The postmark content is assembled at 306. Postmark content as was previously noted may include the message digest, a date time stamp from the secure clock 232, a serial number, and any other desirable data as an option. A determination is made at 308 if sufficient funds exist in the postage and certificate meter subsystem 218 to proceed with the generation of the cryptographic postmark. It should be recognized that these funds may be stored in the descending certificate register, the descending postal register or other registers within the subsystem containing an indication of available funds of the user or party paying for the postmark. If sufficient funds are not available, the request for postmark generation is rejected at 310. If, on the other hand, sufficient funds are available, the funds are deducted for the signing of the assembled postmark content at 312. The postmark content is then signed at 314 to produce a postmark and the message, postmark and certificate are sent to the desired location at 316. This may be a remote facility where it is first communicated through the communications port 234 to the personal computer communication port 216 and thereafter via the processor 212 and modem 220 to the remote facility. Alternatively, the secure (or non-secure) printer of the postage and certificate meter sub unit 218 may print a hard copy of the message, postmark and certificate. This also may be printed on printer 210 of the personal computer. Additionally, the message, postmark and certificate may also be stored in memory 214 of the personal computer 204 and/or memory 226 of the postage and certificate meter 218.

Reference is now made to Figure 3A, a user of the postage certificate meter 218 can act as a certificate agent. For example, a business may wish to issue certificates for their employees. The postage and certificate meter 218 can provide a tool to securely generate the public and private keys. The postage and certificate meter 218 private key can be employed to sign the certificate. Another party who receives the certificate has assurance that the certificate was generated under the authority of the postage certificate meter 218 issued to that business.

The agent sends a request for a certificate to the agent's certificate meter at 350. The request may include any data typically included in a certificate including expiration date, issuing authority, purposes the certificate is authorized for, the unique name of the party the certificate is issue for, and any other data describing allowed or limited uses of the certificate. The certificate meter generates a public and private key pair at 351. The process of generating the key pair is secured in the certificate meter in the key generator of the postage and certificate meter 218. At 354 the private key is sent to the receiver. The private key must be securely communicated to the receiver, for example it may be encrypted, or security measures may be taken to provide assurance that the key is not intercepted. The postage and certificate meter 218 assembles the certificate data at 356. At 358 the certificate meter 218 determines the charge for signing the certificate, and if a determination is made that there is not sufficient funds to pay for signing the certificate data with the agent's certificate meter private key, then the request is rejected at 360. If a determination is made at 358 that there is sufficient funds then funds for signing are deducted at 362 and the certificate is signed at 364 and the certificate sent to the receiver at 366.

Reference is now made to Figure 4 showing the validation of a cryptographic postmark. A request for validation of the postmark is initiated at 402. A determination is made at 404 if sufficient funds are available within the postage and certificate meter subsystem 218. If sufficient funds are not available the request is rejected at 406. If sufficient funds are available the requester utilizes the certificate authority's public key to verify the signature of the certificate at 408 and accounts for it. If the signature is determined not to be valid at 410, the certificate is rejected at 412. If the signature is determined to be valid at 410, a message digest is generated and compared with the decrypted postmark at 414. A determination is made at 416 if the generated message digest and the message digest in the decrypted postmark match. If they do not match the postmark is rejected at 418. If, on the other hand, they do match, the postmark is reported as valid at 420.

Reference is now made to FIGURE 5. A request for installation of the certificate is initiated at 502. A determination is made at 504 if sufficient funds are available in the postage and certificate meter subsystem 218 to

cover the charges associated with processing the request. If sufficient funds are not available the request is rejected at 506. If sufficient funds are available the postage and certificate meter communication key is retrieved at 508. The postage and certificate meter thereafter generates a public and private key pair at 510. Thus, the secure postage and certificate meter subsystem 218 securely generates the private key at 510. Thus, the private key is never available outside of the secure housing of the postage and certificate meter subsystem 218. In this preferred embodiment the private key is not known to anyone, including the certificate owner, therefore the postage and certificate meter can enforce charges for any use of the private key.

If less security is required and depending upon the configuration and needs of the system, the system can be modified such that the user can enter the private key into the postage and certificate meter subsystem 218. The certificate request is communicated to the certificate authority using the certificate communication key at 512. This key is shown at 256 in FIGURE 2.

A determination is made at 514 to whether the user identification has been verified. If the verification fails, the request is rejected at 516. If the identity is verified the certificate generated by certification is received from the authority at 518. Thereafter, the certificate is installed in the postage and certificate meter subsystem 218 via the personal computer modem 220 and processor 212 and communication port 216 to the communication port 234 of the postage and certificate meter subsystem 218. Additionally at 520 the funds are deducted from the postage and certificate meter for the generation and the requested certificate which activates user's private key.

Reference is now made to FIGURE 6 showing the process for revoking an issued certificate. This may occur, for example, where an individual believes that his or her private key has been compromised or as a matter of routine security where private keys are periodically updated and the like. Also, such revocation can occur when the authorization conditions can no longer be obtained and the certificate should, accordingly, be revoked. A request to the certificate authority to revoke a certificate is signed at 602. A verification of the request signature is made at 604. If the verification fails, the revocation request is rejected at 606. If the signature is verified, a signed message is issued to the postage and certificate meter subsystem 218 to revoke the certificate in question at 608. The postage and certificate meter subsystem 218 checks the signature on the revocation response at 610. If the signature fails to be verified at 612, the response issuing the signed message is rejected at 614. If on the other hand, the signature is verified, the postage and certificate meter revokes the certificate at 616. A determination is then made if sufficient funds are available at 618. If sufficient funds are not available a signed confirmation of the revocation and payment due is issued at 620. Thereafter, the revocation time and reason in the certification authority database is entered at 622. Further procedures, not shown may be taken to ensure payment due is in fact received. The handling of debiting the registers for certificate revocation will depend on the nature of the system and certificate involved and this may even be included as part of the certificate itself.

If at 618 sufficient funds are available, the signed confirmation of revocation and payment is issued at 624. This is entered into the certificate authority database at 622.

The process described in FIGURE 6 may be adapted for a forced revocation of due certificate, for a example by the certification authority or its agent . In this case, at the contract with the certification authority or during inspection process due revocation starts at 608. The payment at 624 can be disabled. If no contact is made the certificate meter will either run out of money or timed out after a prespecified time period.

Reference is now made to FIGURE 7A. A line of credit certificate 702 is shown as an example of one type of credit certificate. This certificate similar to the certificate shown in FIGURE 1 includes the name of the individual receiving credit at 704, the serial number or unique identifier of the certificate at 706 and the public key of the creditor (person receiving credit) may preferably be included at 708. The credit issuer identification may be included at 710 as well as the credit line amount at 712, the validity dates at 714 and the authorized use at 716. Also included in the certificate is the credit issuer signature 718. The creditor private key is shown at 720 and is securely maintained by the creditor.

It should be noted that the name at 704 as well as the name in various other certificates shown in the present application is in fact a unique identifier and may be a number or other identifying data of the certificate holder.

Reference is now made to FIGURE 7B which is another example of a certificate, here a payment certificate which is related to the line of credit certificate shown in 7A. The certificate shown generally at 722 may include the name of the certificate holder at 724, unique identification or serial number at 726, meter identification at 728, digest of line of credit certificate at 730, amount authorized at 731, credit remaining at 732 and, finally, the postage and certificate meter signature at 734. The user private key associated with the signature is shown at 736 and is treated as confidential and protected information.

Reference is now made to FIGURE 8 showing the process for receiving a line of credit. The request for credit with postage and certificate meter postmark is initiated at 802. The creditor determines whether to issue credit at 804. If the credit check fails, the creditor rejects the request at 806. If the credit check passes, the creditor generates the line of credit certificate at 808. The line of credit is received by the requester at 810 and an initial payment certificate with credit remaining equal to

the full line of credit can be created at 812. This certificate is stored in the postage and certificate meter subsystem 218 memory 226.

Reference is now made to FIGURE 9 showing payment from a issued line of credit. A request for payment from the line of credit is initiated at 902. This request may be initiated by the user of the postage and certificate meter 218 as part of a transaction purchasing goods or services. If sufficient funds are determined to be not available at 904 the request is rejected at 906. If, on the other hand, sufficient funds are determined to be available at 904, the payment amount is subtracted from the credit remaining at 908 and a payment certificate is created at 910. In this manner a payment certificate is created and provided to the merchant evidencing the availability of funds to pay for the transaction and enables the merchant who receives and authenticates the payment certificate to receive funds from the requester's bank. The merchant delivers the merchandise and sends a copy of the payment certificate to the party who provided the credit to the user of the postage and certificate meter subsystem 218. This is evidence of authorization by the user and authorizes the issuer of credit to pay the merchant. This constitutes the proof of request of payment and constitutes an authorization by the user to have payment issued to the merchant. While the present invention has been disclosed and described with reference to the disclosed embodiments thereof, it will be apparent, as noted above, that variations and modifications may be made.

It should be recognized that the present invention provides a mechanism for the active forceful revocation of the certificate itself so that the certificate holder cannot reuse the certificate. This is for several reasons. The funding registers periodically must be serviced. For ascending/descending register systems, the recharging process where funds are added require communications with the trusted third party at which time the revocation can be implemented Moreover, as noted above, in certain countries meters are leased and owned by the manufacturer thereby giving legal access to the meter. For current account systems, failure to service the meter can cause the meter to lock up. Various lock ups and time outs can also be included in the meter to preclude further operation of the system. Additionally, by virtue of the utilization of the postage or value metering including postage metering devices, inherent advantages in the postage metering system such as inspections, security, trusted third party (postal authority) become available to utilize for enhanced security.

While the present invention has been disclosed and described with reference to the disclosed embodiments thereof, it will be apparent that many various and modifications may be made. For example when a user needs to verify a certificate obtained from another party, the user needs to have access to the public key of the trusted third party certification authority that signed the certificate in question. This can be done by storing the certification authority's public key in the postage and certificate meter and updating this key when needed by using communication parts 234 and 216 (Fig. 2) or by entering this key manually via personal computer 204. As another example, the postage meter and certificate meter subsystem may be implemented as a smart card or as a computer card peripheral or internal circuit board or as a computer PCMCIA card, also known as PC card. Thus, it is intended in the following claims to cover each variation and modification that falls within the true spirit and scope of the present invention.

Claims

1. A system, comprising:

   register means;

   means for processing a cryptographic certificate adapted to provide security functionality; and,

   means operatively connected to said register means and said processing means for adjusting said register means to account for services when said cryptographic certificate is processed.

2. A system as defined in CLAIM 1 wherein said register means have funds stored therein and said means for adjusting debits funds stored in said register means when said cryptographic certificate is processed.

3. A system as defined in CLAIM 1 or 2 further comprising means for inhibiting processing of said cryptographic certificate when funds stored in said register means are below a predetermined amount associated with processing said cryptographic certificate.

4. A system as defined in any preceding CLAIM further comprising a secure housing, said means for processing a certificate are mounted within said secure housing.

5. A system defined in any preceding CLAIM wherein said means for processing a cryptographic certificate has cryptographic key means.

6. A system as defined in CLAIM 5 wherein said cryptographic key means includes a private key for use in a public key system.

7. A system as defined in CLAIM 6 wherein said cryptographic key means further includes a public key associated with said private key, said public key be-

ing signed with the private key of a certification authority and said public key being available to a user of the system.

8. A system as defined in any one of claims 5 to 7, further comprising communications means coupled to said means for processing a cryptographic certificate for providing means for communicating cryptographic key information for storage in said cryptographic key means.

9. A system as defined in CLAIM 8 wherein said means for communicating is mounted within said secure housing and provides a communication path from outside said secure housing to within said secure housing.

10. A system as defined in CLAIM 8 or 9 further comprising an input means coupled to said communications means for inputting data into said system.

11. A system as defined in CLAIM 10 wherein said input means is a personal computer means, said personal computer means including modem means for enabling communications with a remote location and enabling communications from said remote location to said communications means for entering data into said system from said remote location.

12. A system as defined in any preceding CLAIM wherein said means for processing a cryptographic certificate includes means for generating a cryptographic certificate.

13. A system as defined in any preceding CLAIM where said means for processing of a cryptographic certificate includes means for verifying a cryptographic certificate.

14. A system as defined in any preceding CLAIM wherein said means for processing cryptographic certificates includes key generator means.

15. A system as defined in any preceding CLAIM further including recharging means coupled to said register means to enable funds stored in said register means to be remotely recharged with additional funds.

16. A system as defined in any preceding CLAIM wherein said adjusting means includes a table of charges for a plurality of services capable of being provided when said cryptographic certificate is processed.

17. A system, comprising:

register means for storing funds;

means for processing a digital token providing proof of postage payment;

means for processing a cryptographic certificate adapted to provide security functionality; and,

means, operatively connected to said register means and to said means for processing a digital tokens and to said means for processing a certificate, for debiting funds stored in said register means when said digital token is processed and when said cryptographic certificate is processed.

18. A system as defined in CLAIM 17 further comprising means operatively connected to said register means for inhibiting the processing of said digital token when the funds stored in said register means are below a predetermined amount associated with processing of said digital token and for inhibiting processing of said cryptographic certificate when the funds stored in said register means are below a predetermined amount associated with processing said cryptographic certificate.

19. A system defined in CLAIM 17 or 18 wherein said means for processing a digital token has first cryptographic key means and said means for processing a cryptographic certificate has second cryptographic key means.

20. A system as defined in any one of claims 17 to 19 further comprising a secure housing, said means for processing a digital token and said means for processing a cryptographic certificate mounted within said secure housing.

21. A system as defined in any one of claims 17 to 20 wherein said first cryptographic key means includes a secret key for use in secret key encryption system and said second cryptographic key means includes a private key for use in a public key encryption system.

22. A system as defined in CLAIM 21 wherein said second cryptographic key means further includes a public key associated with said private key, said public key being signed with the private key of a certification authority.

23. A system as defined in CLAIM 22 as dependent on claim 19 further comprising communications means coupled to said means for processing a digital token and said means for processing a cryptographic certificate for providing a communications path for communicating cryptographic key information for storage in said first cryptographic key means and in

said second cryptographic key means.

24. A system as defined in CLAIM 23 as dependent on claim 20 wherein said means for communicating is mounted within said secure housing and said communication path enables communications from outside said secure housing to within said secure housing.

25. A system as defined in CLAIM 24 further comprising an input means coupled to said communications means for inputting data into said system.

26. A system as defined in CLAIM 25 wherein said input means is a personal computer means, said personal computer means including modem means for enabling communications with a remote location and enabling communications from said remote location to said communications means for entering data into said system from said remote location.

27. A system as defined in any of claims 17 to 26 wherein said means for processing a cryptographic certificate includes generating said cryptographic certificate.

28. A system as defined in any of claims 17 to 27 where said processing of said cryptographic certificate comprises verifying said cryptographic certificate.

29. A system defined in any one of claims 17 to 28 further comprising a plurality of further means for processing cryptographic certificates.

30. A system as defined in any one of claims 17 to 29 further including recharging means coupled to said register means to enable funds stored in said register means to be remotely recharged with additional funds.

31. A system as defined in any one of claims 17 to 30 wherein said means for processing a digital token includes generating said digital token.

32. A system, comprising:

register means;

means for processing a digital token providing proof of postage payment;

means for processing a cryptographic certificate adapted to provide security functionality; and,

means, operatively connected to said means for processing a digital token and to said means for processing a cryptographic certificate, for adjusting said register means to account for services when said cryptographic certificate is processed and when said digital token is processed.

33. A method for use in a system having a register means, comprising:

processing a cryptographic certificate adapted to provide security functionality; and,

adjusting said register means to account for services when said cryptographic certificate is processed.

34. A method for use in a system having register means for storing funds, comprising:

processing a digital token providing proof of postage payment;

processing a cryptographic certificate adapted to provide security functionality; and,

debiting funds stored in said register means when said digital token is processed and when said cryptographic certificate is processed.

FIG. 2

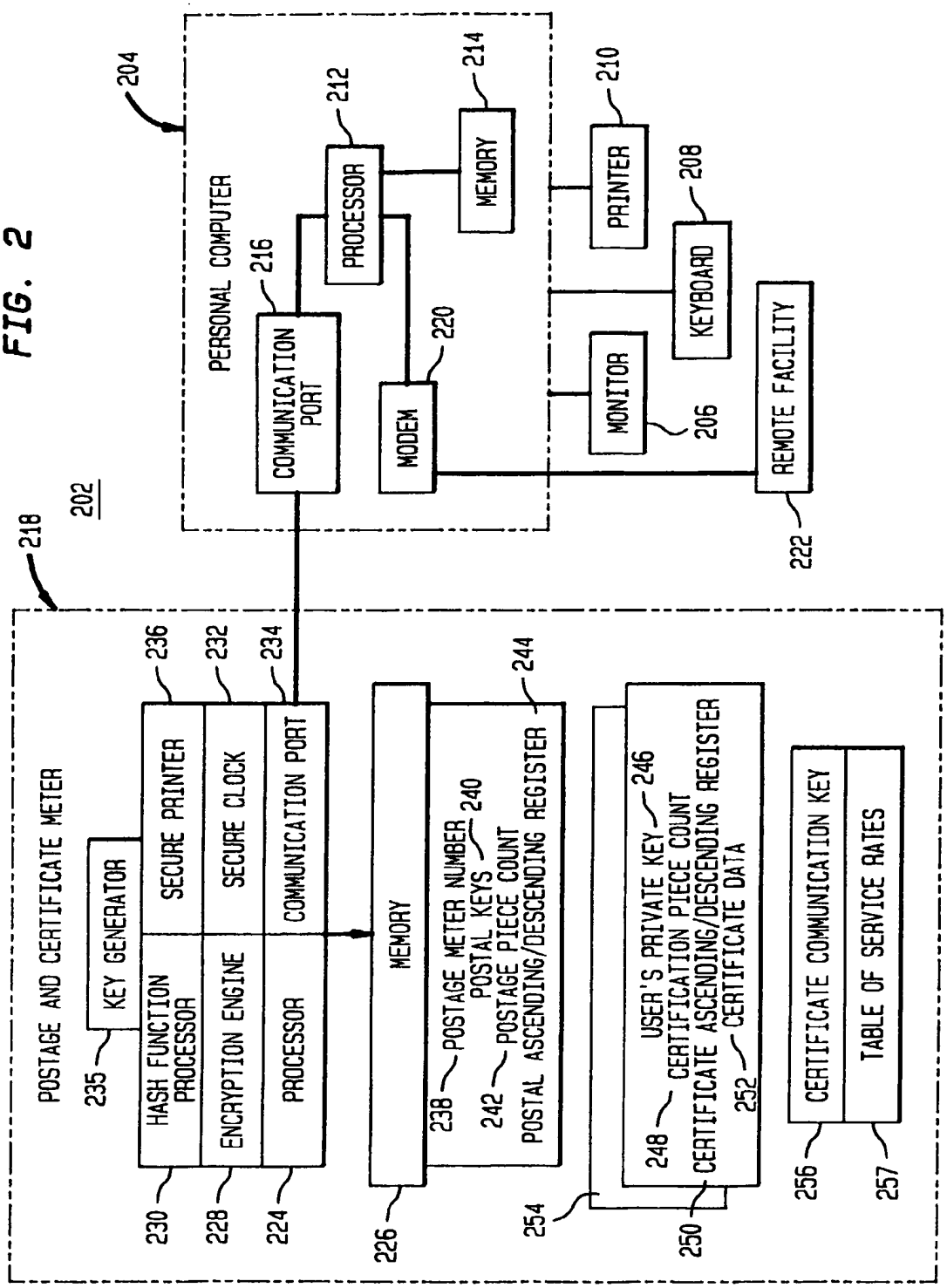

202
204
PERSONAL COMPUTER
PROCESSOR
212
MEMORY
214
PRINTER
210
KEYBOARD
208
COMMUNICATION PORT
216
MODEM
220
MONITOR
206
REMOTE FACILITY
222
218
POSTAGE AND CERTIFICATE METER
KEY GENERATOR
235
HASH FUNCTION PROCESSOR
230
ENCRYPTION ENGINE
228
PROCESSOR
224
SECURE PRINTER
236
SECURE CLOCK
232
COMMUNICATION PORT
234
MEMORY
226
POSTAGE METER NUMBER
238
POSTAL KEYS
240
POSTAGE PIECE COUNT
242
POSTAL ASCENDING/DESCENDING REGISTER
244
254
USER'S PRIVATE KEY
246
CERTIFICATION PIECE COUNT
248
CERTIFICATE ASCENDING/DESCENDING REGISTER
CERTIFICATE DATA
252
250
CERTIFICATE COMMUNICATION KEY
256
TABLE OF SERVICE RATES
257

FIG. 1

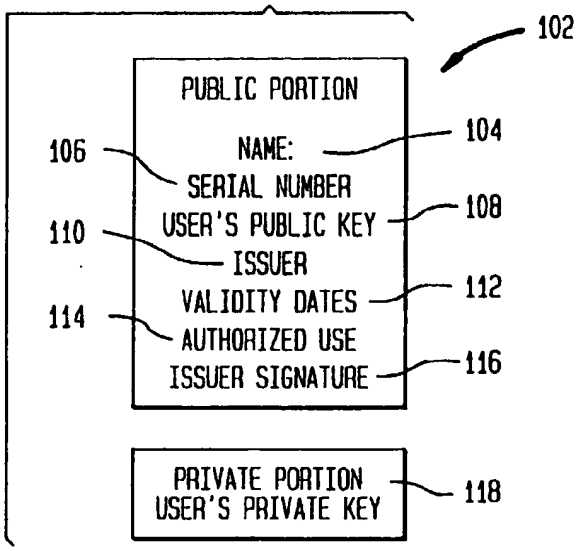

102
PUBLIC PORTION
NAME:
104
106
SERIAL NUMBER
USER'S PUBLIC KEY
108
110
ISSUER
VALIDITY DATES
112
114
AUTHORIZED USE
ISSUER SIGNATURE
116
PRIVATE PORTION
USER'S PRIVATE KEY
118

FIG. 3

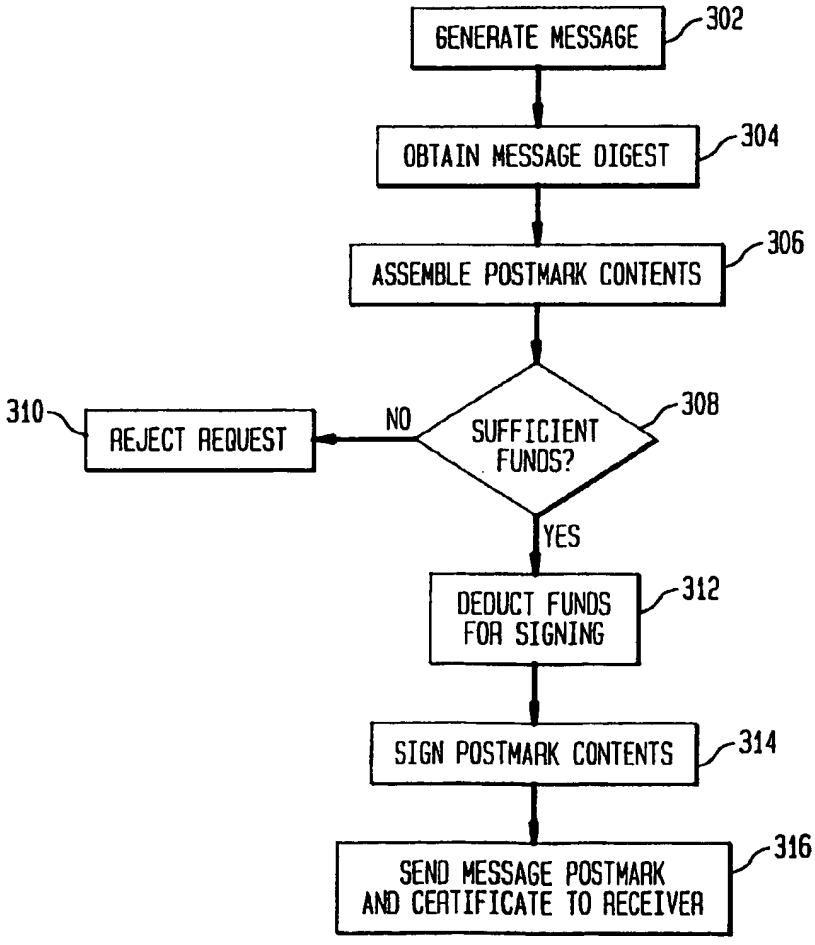

GENERATE MESSAGE
302
OBTAIN MESSAGE DIGEST
304
ASSEMBLE POSTMARK CONTENTS
306
SUFFICIENT FUNDS?
308
NO
310
REJECT REQUEST
YES
DEDUCT FUNDS FOR SIGNING
312
SIGN POSTMARK CONTENTS
314
SEND MESSAGE POSTMARK AND CERTIFICATE TO RECEIVER
316

FIG. 3A

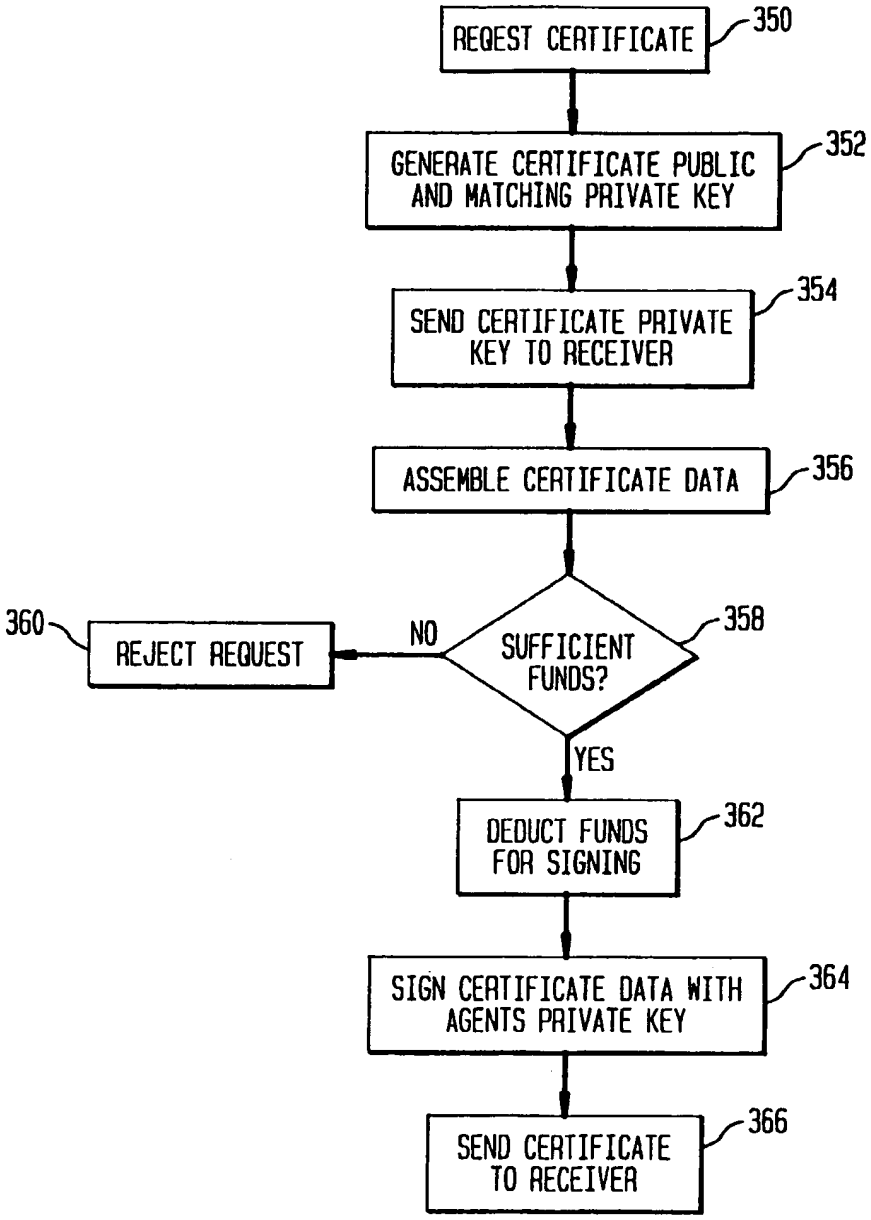

REQEST CERTIFICATE
350
GENERATE CERTIFICATE PUBLIC AND MATCHING PRIVATE KEY
352
SEND CERTIFICATE PRIVATE KEY TO RECEIVER
354
ASSEMBLE CERTIFICATE DATA
356
SUFFICIENT FUNDS?
358
NO
360
REJECT REQUEST
YES
DEDUCT FUNDS FOR SIGNING
362
SIGN CERTIFICATE DATA WITH AGENTS PRIVATE KEY
364
SEND CERTIFICATE TO RECEIVER
366

FIG. 4

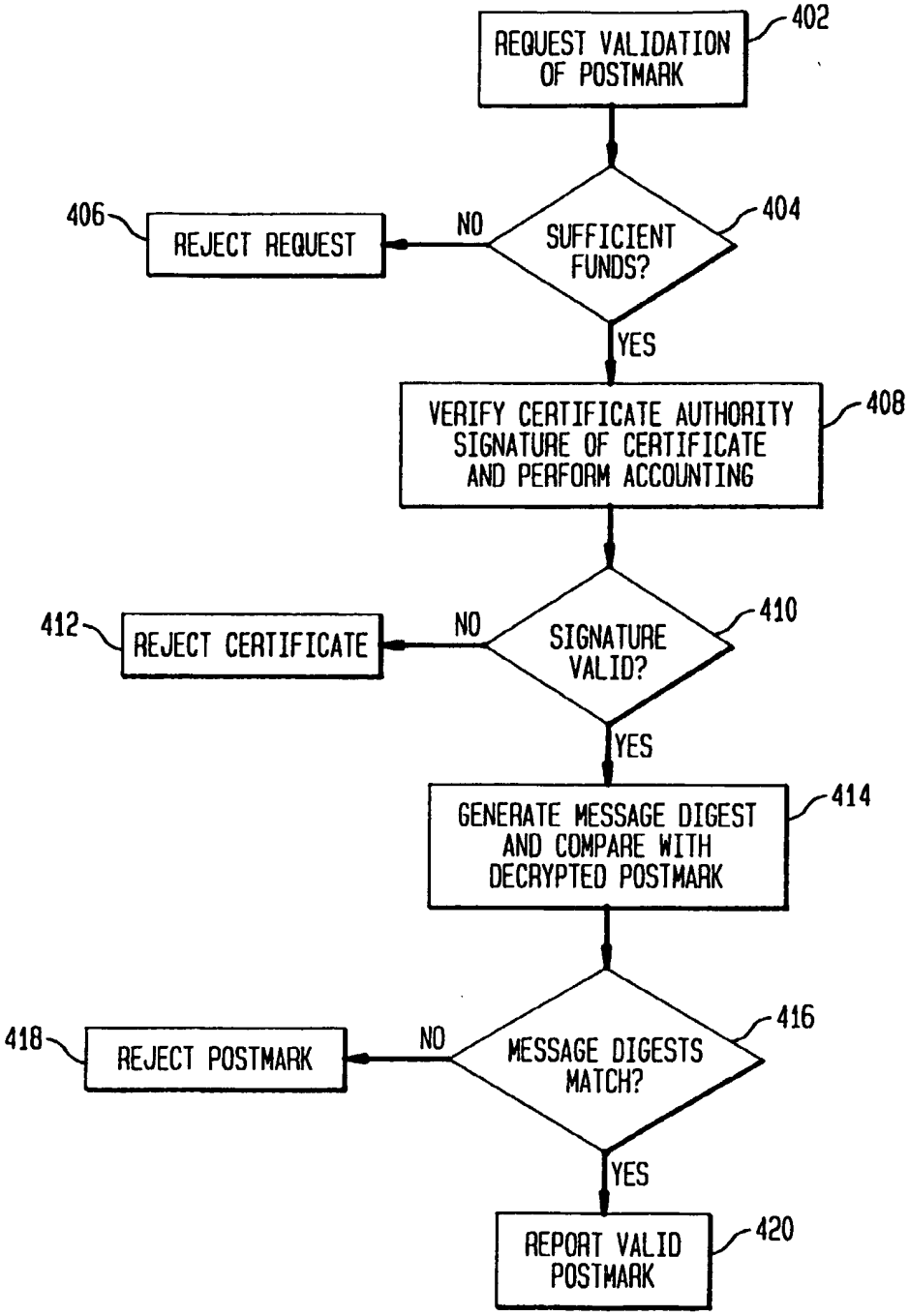

REQUEST VALIDATION OF POSTMARK
402
SUFFICIENT FUNDS?
404
NO
406
REJECT REQUEST
YES
VERIFY CERTIFICATE AUTHORITY SIGNATURE OF CERTIFICATE AND PERFORM ACCOUNTING
408
SIGNATURE VALID?
410
NO
412
REJECT CERTIFICATE
YES
GENERATE MESSAGE DIGEST AND COMPARE WITH DECRYPTED POSTMARK
414
MESSAGE DIGESTS MATCH?
416
NO
418
REJECT POSTMARK
YES
REPORT VALID POSTMARK
420

FIG. 5

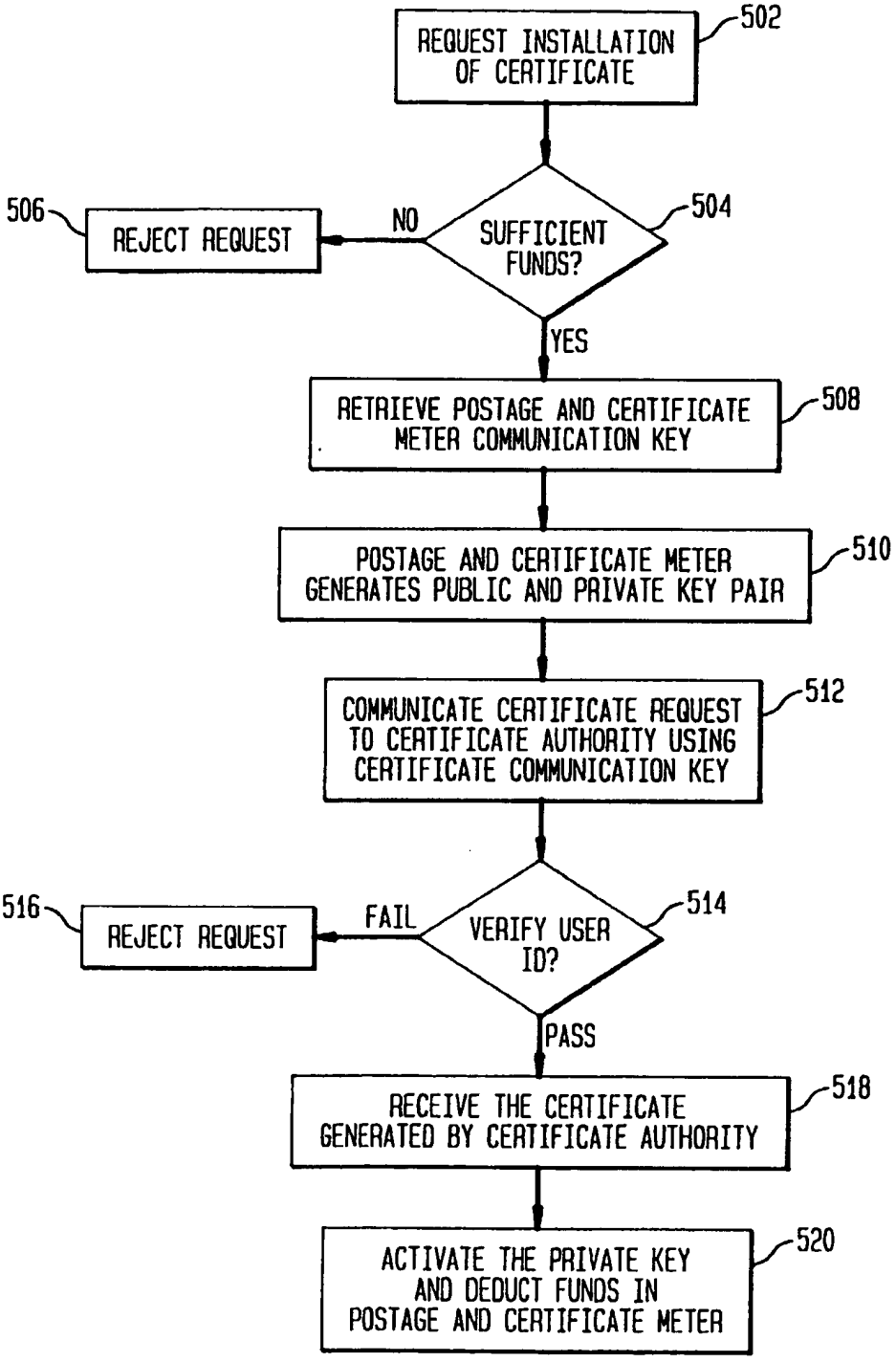

REQUEST INSTALLATION OF CERTIFICATE
502
SUFFICIENT FUNDS?
504
NO
506
REJECT REQUEST
YES
RETRIEVE POSTAGE AND CERTIFICATE METER COMMUNICATION KEY
508
POSTAGE AND CERTIFICATE METER GENERATES PUBLIC AND PRIVATE KEY PAIR
510
COMMUNICATE CERTIFICATE REQUEST TO CERTIFICATE AUTHORITY USING CERTIFICATE COMMUNICATION KEY
512
VERIFY USER ID?
514
FAIL
516
REJECT REQUEST
PASS
RECEIVE THE CERTIFICATE GENERATED BY CERTIFICATE AUTHORITY
518
ACTIVATE THE PRIVATE KEY AND DEDUCT FUNDS IN POSTAGE AND CERTIFICATE METER
520

FIG. 6

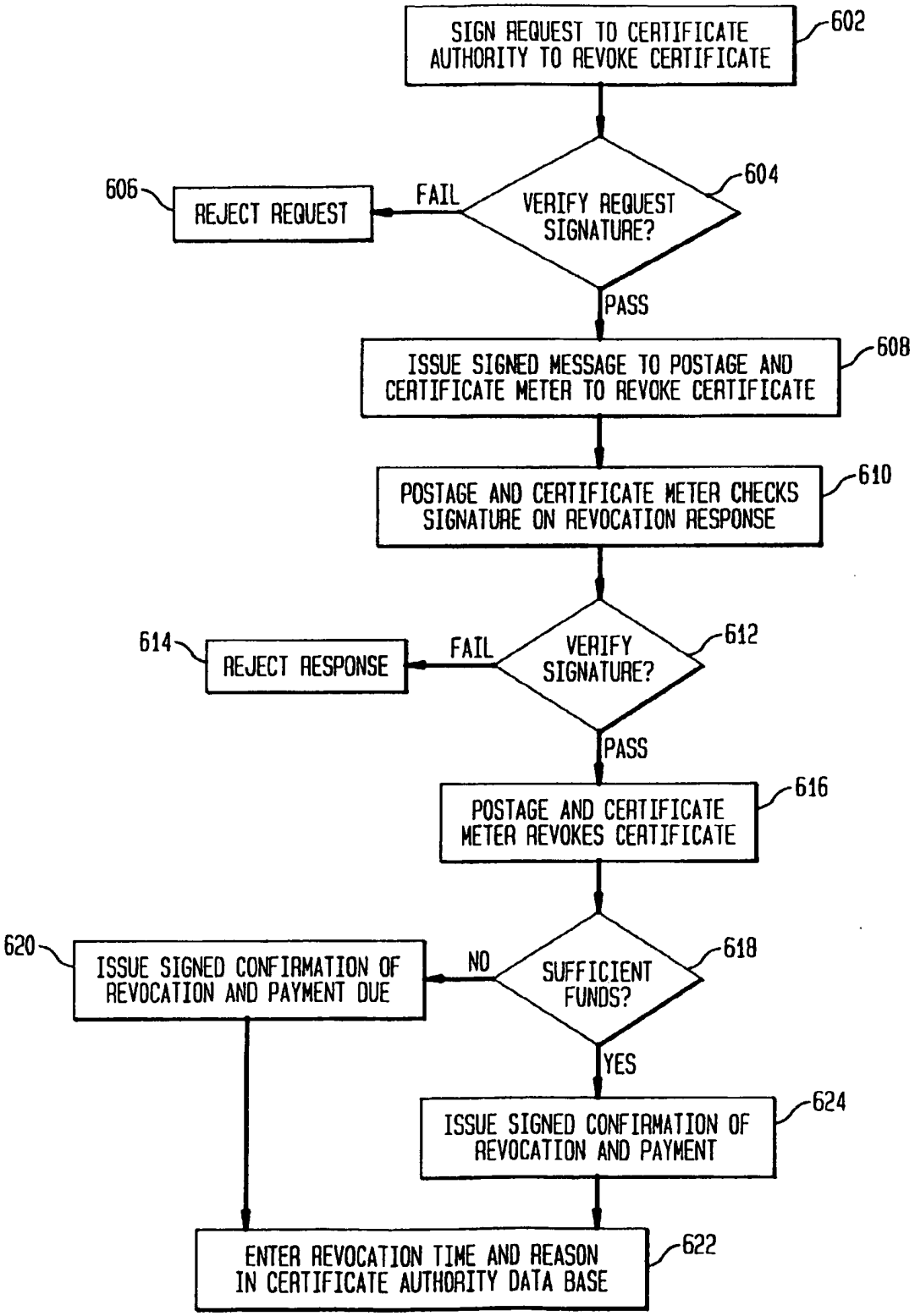

SIGN REQUEST TO CERTIFICATE AUTHORITY TO REVOKE CERTIFICATE
602
VERIFY REQUEST SIGNATURE?
604
FAIL
REJECT REQUEST
606
PASS
ISSUE SIGNED MESSAGE TO POSTAGE AND CERTIFICATE METER TO REVOKE CERTIFICATE
608
POSTAGE AND CERTIFICATE METER CHECKS SIGNATURE ON REVOCATION RESPONSE
610
VERIFY SIGNATURE?
612
FAIL
REJECT RESPONSE
614
PASS
POSTAGE AND CERTIFICATE METER REVOKES CERTIFICATE
616
SUFFICIENT FUNDS?
618
NO
ISSUE SIGNED CONFIRMATION OF REVOCATION AND PAYMENT DUE
620
YES
ISSUE SIGNED CONFIRMATION OF REVOCATION AND PAYMENT
624
ENTER REVOCATION TIME AND REASON IN CERTIFICATE AUTHORITY DATA BASE
622

FIG. 7A

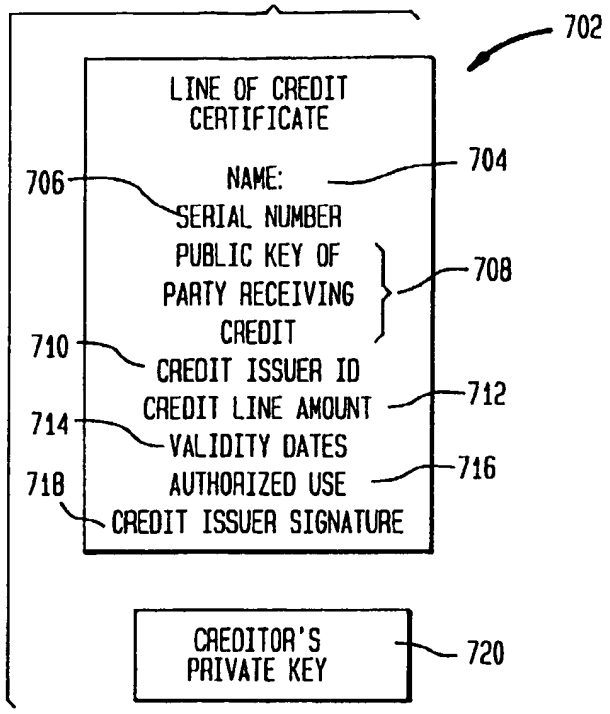

LINE OF CREDIT CERTIFICATE
NAME:
SERIAL NUMBER
PUBLIC KEY OF PARTY RECEIVING CREDIT
CREDIT ISSUER ID
CREDIT LINE AMOUNT
VALIDITY DATES
AUTHORIZED USE
CREDIT ISSUER SIGNATURE
CREDITOR'S PRIVATE KEY
702
704
706
708
710
712
714
716
718
720

FIG. 7B

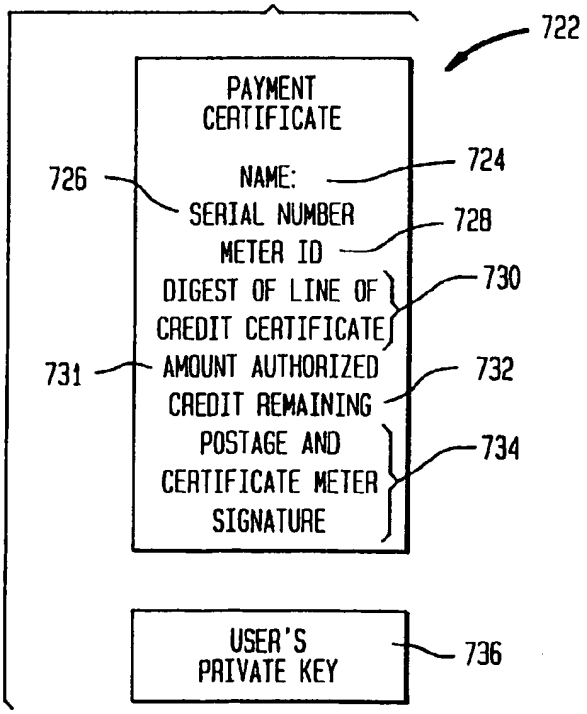

PAYMENT CERTIFICATE
NAME:
SERIAL NUMBER
METER ID
DIGEST OF LINE OF CREDIT CERTIFICATE
AMOUNT AUTHORIZED
CREDIT REMAINING
POSTAGE AND CERTIFICATE METER SIGNATURE
USER'S PRIVATE KEY
722
724
726
728
730
731
732
734
736

FIG. 8

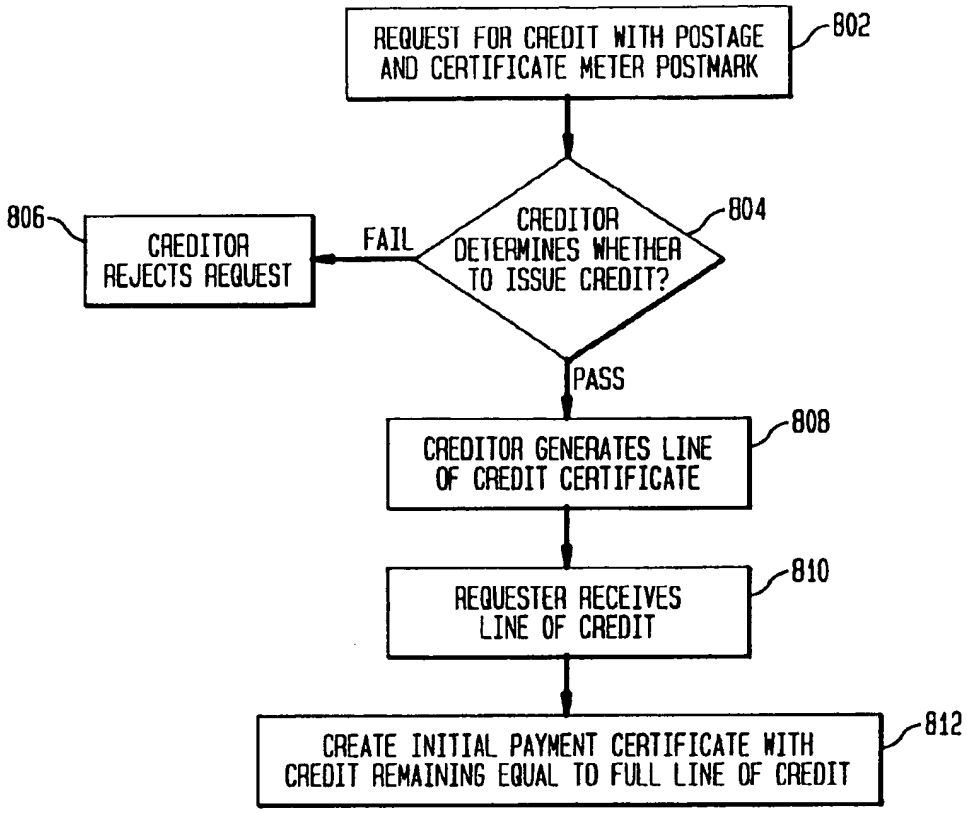
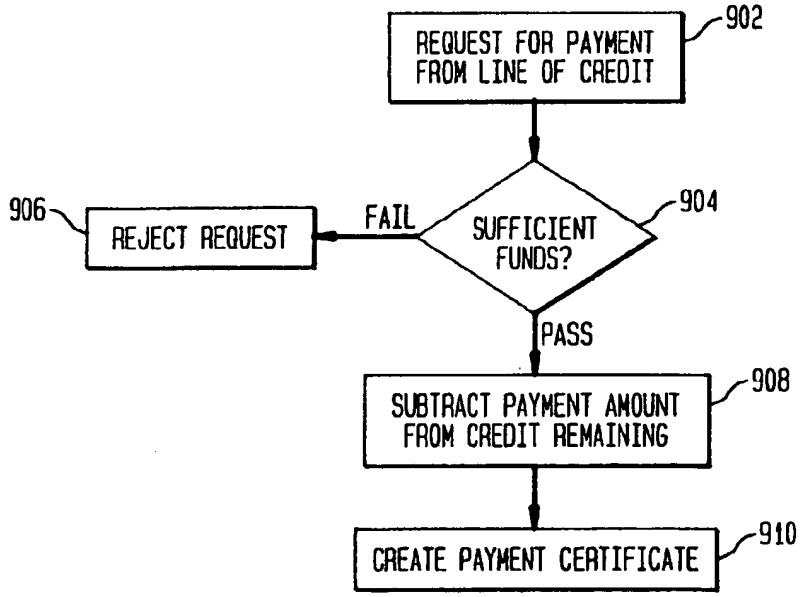

REQUEST FOR CREDIT WITH POSTAGE AND CERTIFICATE METER POSTMARK
802
CREDITOR DETERMINES WHETHER TO ISSUE CREDIT?
804
FAIL
806
CREDITOR REJECTS REQUEST
PASS
CREDITOR GENERATES LINE OF CREDIT CERTIFICATE
808
REQUESTER RECEIVES LINE OF CREDIT
810
CREATE INITIAL PAYMENT CERTIFICATE WITH CREDIT REMAINING EQUAL TO FULL LINE OF CREDIT
812

FIG. 9


REQUEST FOR PAYMENT FROM LINE OF CREDIT
902
SUFFICIENT FUNDS?
904
FAIL
906
REJECT REQUEST
PASS
SUBTRACT PAYMENT AMOUNT FROM CREDIT REMAINING
908
CREATE PAYMENT CERTIFICATE
910